



Chris C. Kemp

STANDARDS, NEBULA AND INTEROPERABILITY

Part 1: NASA's View of Cloud

Why is NASA focused on cloud?

- Many, many, many websites
- Many, many, many different platforms
- Very high operating cost
- Long provisioning times
- Very large attack surface
- Confusing to outside users
- Lock-in, portability, and interoperability issues

More reasons...

- Missions are focused on the Mission
- Scientists are focused on the Science
- Large-scale infrastructure requirements
- Too much is spent on infrastructure
- Missions Completely Fail (OCO)
- Missions Completely Succeed (Rovers)
- Politics impact Missions (Triana)

NIST Definition of Cloud

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

5 Cloud Attributes

- ⦿ Service-based
- ⦿ Scalable and elastic
- ⦿ Shared
- ⦿ Metered by Use
- ⦿ Uses Internet Technologies

Excerpts from Gartner's "Five Attributes of Cloud Computing"

Service-based

- ⦿ Abstracted from the implementation
- ⦿ Completely automated
- ⦿ Near real-time delivery (seconds or minutes)

Scalable and Elastic

- ⦿ Resources are drawn from a common pool
- ⦿ Dynamically allocated to meet demand
- ⦿ Dynamically released when appropriate
- ⦿ Fully automated

Shared

- ⦿ Common resources build economies of scale
- ⦿ Common infrastructure runs at high efficiency

Metered by Use

- ① Consumers pay for services used
- ① Underlying hardware costs are irrelevant

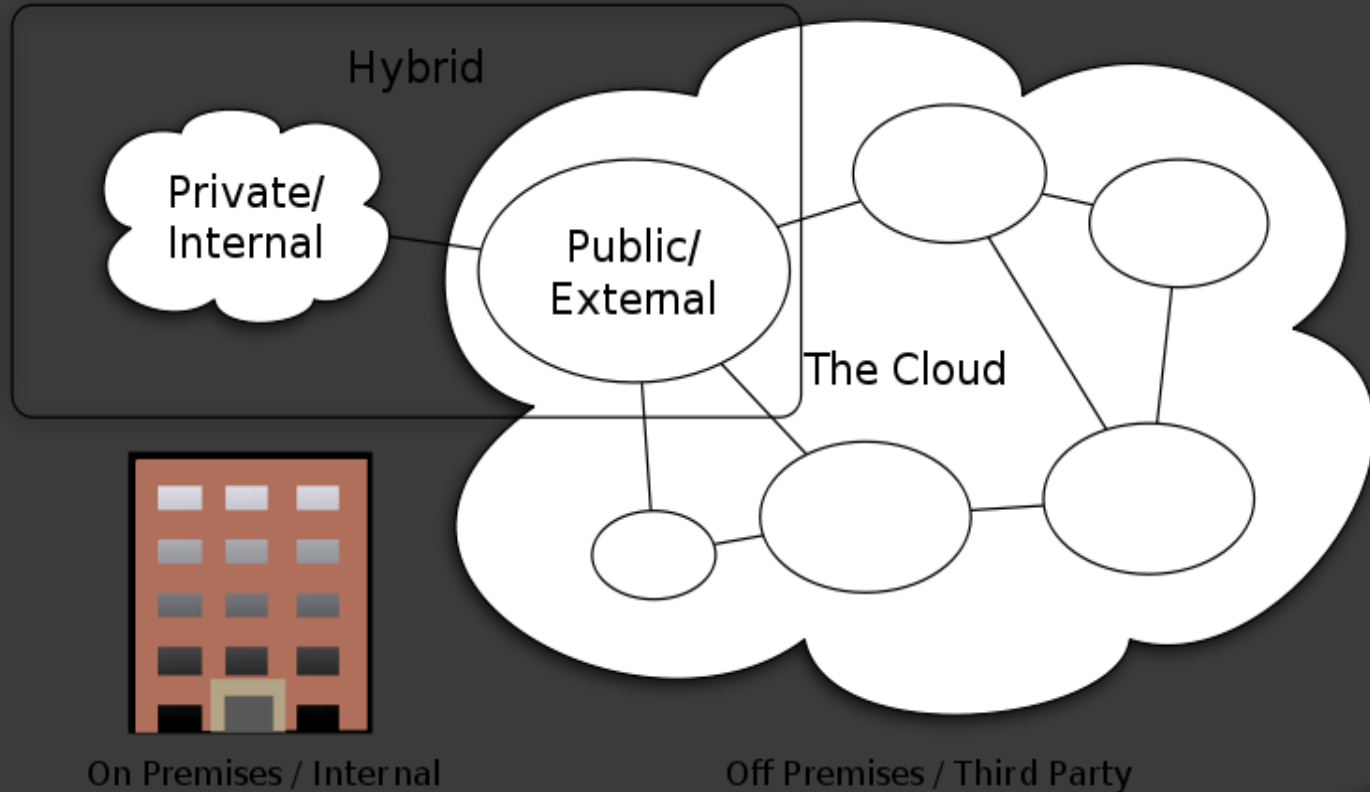
Uses Internet 'Standards'

- ⦿ Open standards and APIs
- ⦿ Almost always IP, HTTP, and REST

Part 2: Nebula



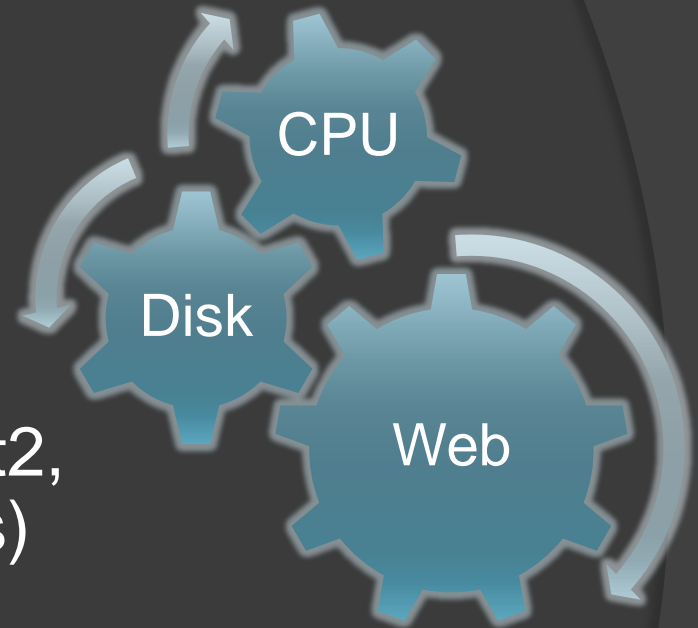
Nebula: A Hybrid Cloud



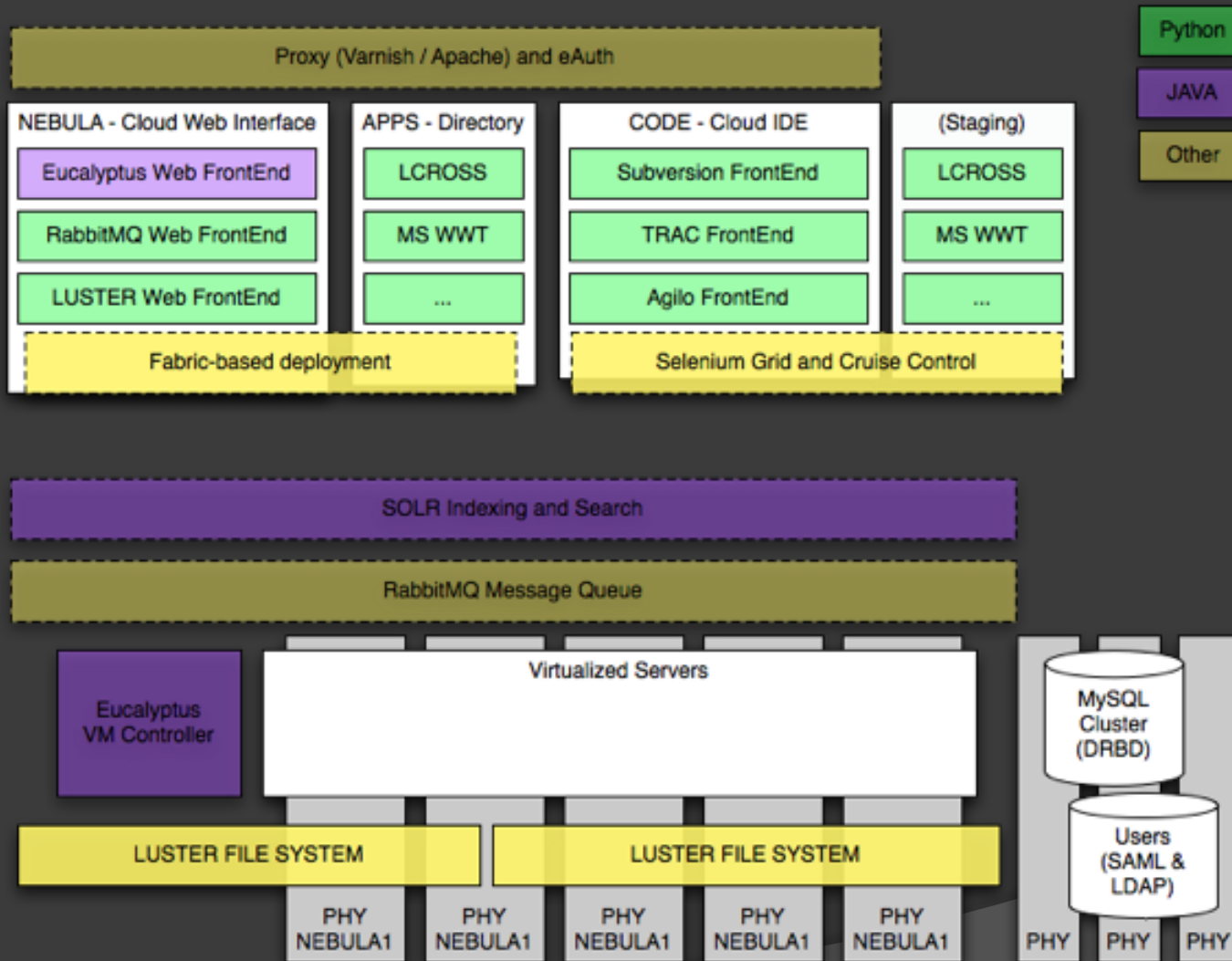
Cloud Computing Types

Built for Science

- ◎ Science-Class Cloud Computing
 - High CPU-to-Disk Ratio
- ◎ Built for Research
 - MAE-West Peering (Internet2, NLR, CENIC, 11 Tier-1 ISPs)
 - Massively Parallel, Loosely Coupled
- ◎ In a Federal Security Perimeter



Nebula Architecture



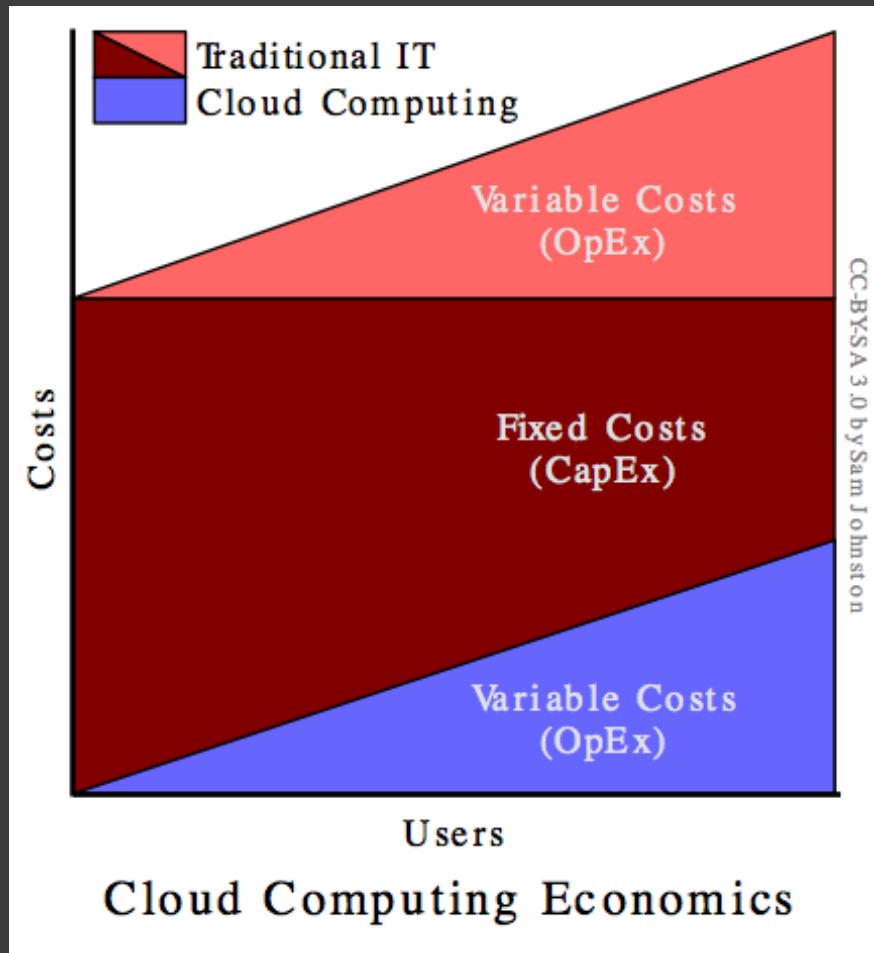
Cloud Platforms, Compared

	AWS	AppEngine	Nebula
Storage	S3, EBS	SimpleStorage API	Luster
Database	SimpleDB	CouchDB	MySQL
Queue	SQS	--	RabbitMQ
Virtualization	EC2 (Xen)	--	Eucalyptus (KVM)
Framework	--	Django	Django
User Accounts	--	Google Accounts	eAuth
Search	--	Google Search	SOLR+Lucene
Networking	1GigE	1GigE	10GigE+
CDN/Cache	CloudFront		Varnish

Application Time to Market

Current Web App Process	NEBULA Cloud Platform
Procure Server – 6-12 weeks	Procure VM – 60-120 seconds
Configure Server – 2-3 days	Included.
AWRS Filing – 2-3 days	Already done. (APPS.NASA.GOV)
Set up Source Control – 2-3 hours.	Included.
Security Plan – 3 weeks, min.	Included.
SSL Certificates – 2-4 weeks.	Included.
Develop Terms of Use – 6 months.	Included, for most collaboration.
eAuth Integration – 40 hours.	Included.
Develop Processes – 3-6 weeks.	Basic moderation included.
Set up backups – 2-3 hours.	Included.
24,192,000 Seconds.	60-120 Seconds.

Must insert budget wedges now!



Built for Collaboration

- True Single-Sign-On, for the Public
- Enterprise Search, across the Cloud
- All Cloud apps live at apps.nasa.gov

Built for the Web

- Friendly URLs
- Designed for Search Engines, RSS, and aggregation
- Components are RSSable, Tweetable
- What if NASA was on the first page of Google results for the term 'Space'?

Built for Partners

- Your science partners can instantly connect from your NEBULA app, to their own research tasks within public Cloud Services (EC2, Azure, AppEngine)
- Your private fleet of Post-Docs can work on your data – at 10 cents an hour

Built for Government

- Policy compliant for contributions
- Consolidated moderation interface
- Everything-compliant (PII, First Amendment, COPPA, Section 508, etc)

Built for Developers

- Integrated Development Environment
- Revision control
- Automated testing
- Continuous Integration
- Bug tracking

Built for Community

- ⦿ Cloud means Turnkey
- ⦿ Dedicated Platform Staff
- ⦿ Engaged External Partners
- ⦿ Common KB shares code, tricks, tips

Nebula - the way to Data.gov

- Best practices in moderation, open collaboration
- Open and Public APIs, everywhere
- Feeds (RSS, Atom) power mash-ups
- Open-source platform, apps, and data
- Full transparency

Pilot Projects

- White House USASpending.gov 2.0
- Microsoft World Wide Telescope (Mars / Moon)
- Google Earth Planetary Content (Mars)
- LMMP Program Data Processing (Moon)
- TOPS Earth Climate Modeling

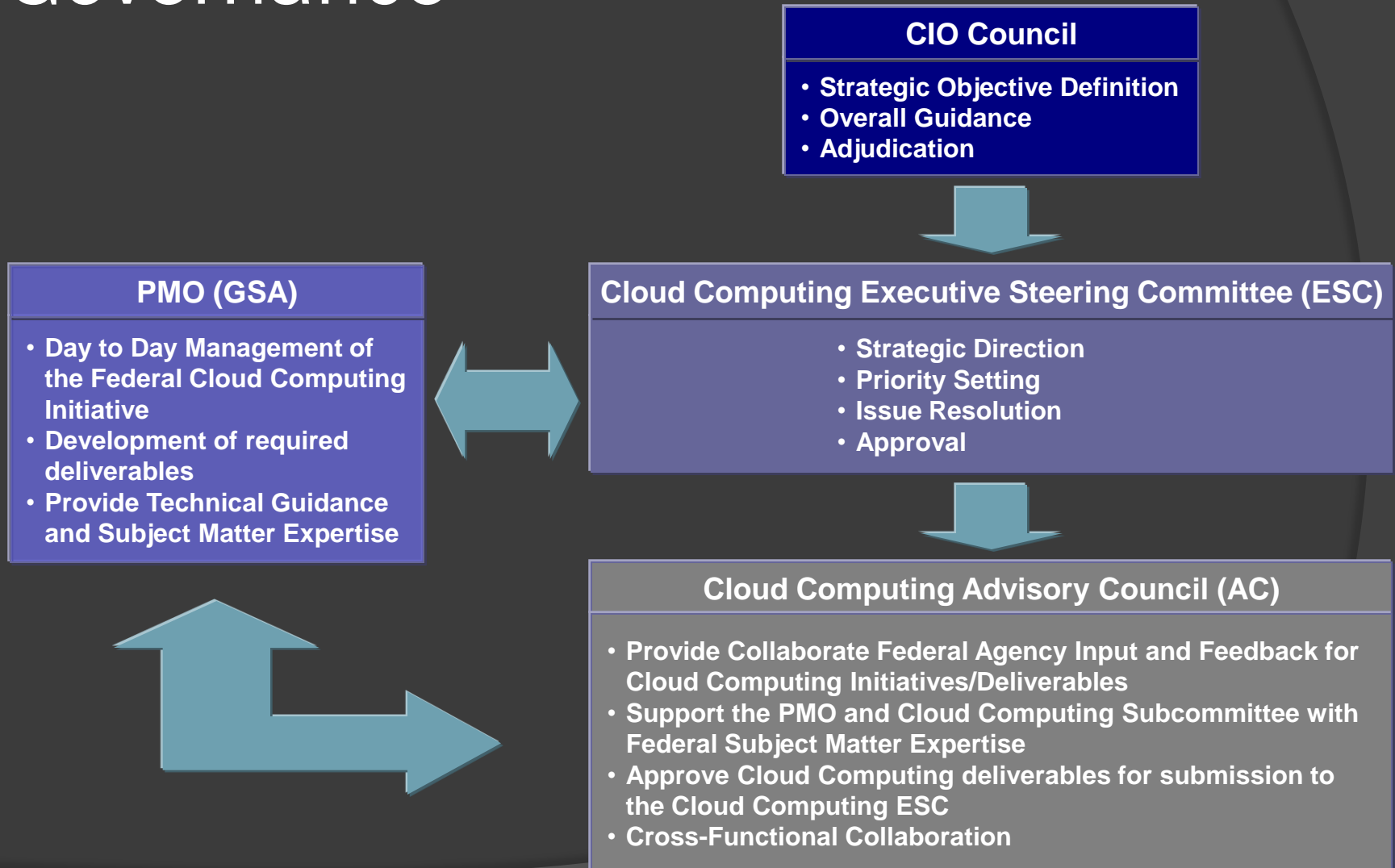


Nebula Timeline

- Under development since May 2008
- Pilot projects underway now
- Full Launch, Q2 2010 (in Apps.gov)
- Concurrent Open Source Release of Code

Part 3: Federal Standards

Federal Cloud Computing Governance



Cloud Standards Working Group

- CC Advisory Council Mission Statement:

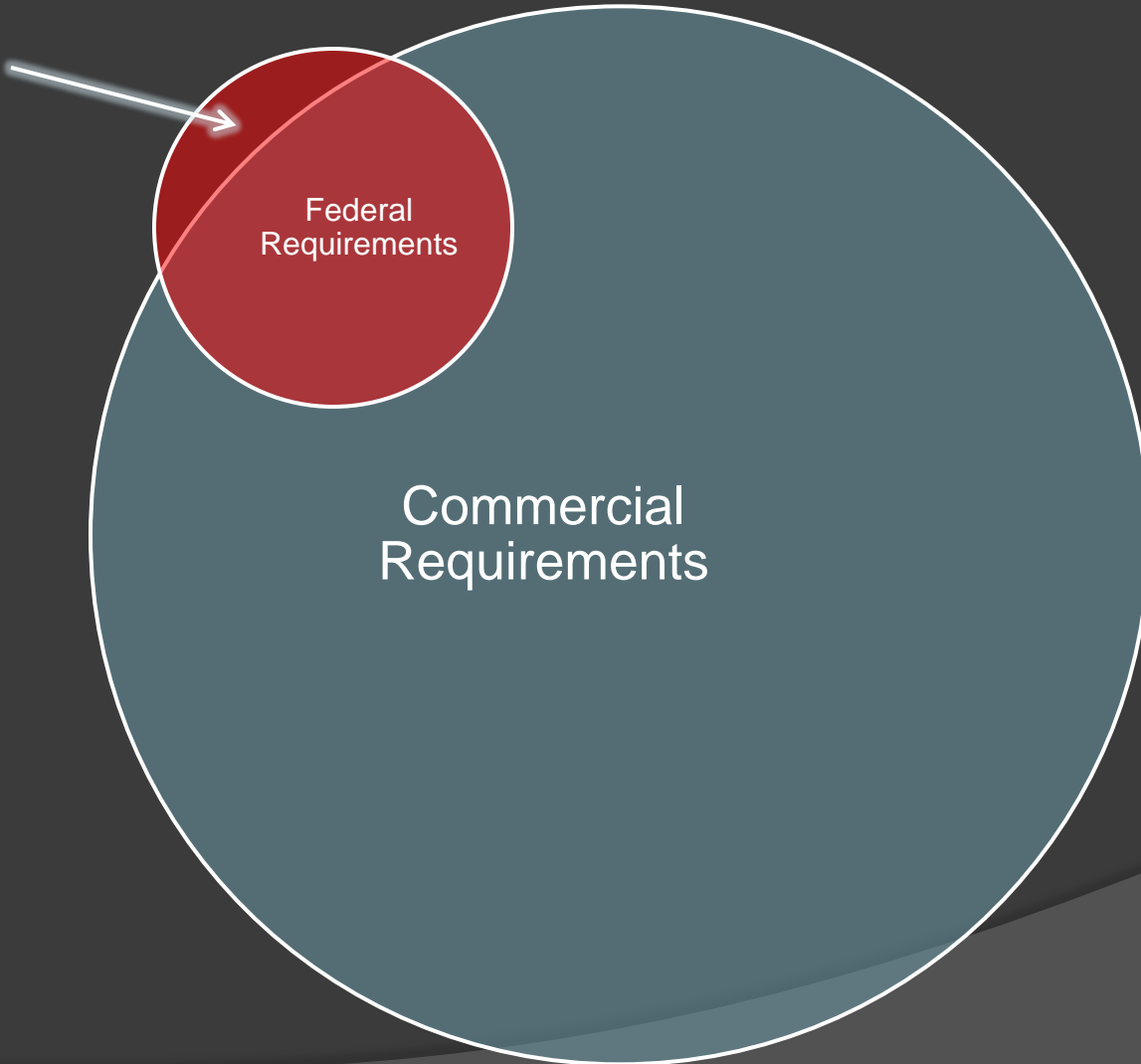
Drive the government-wide adoption of cost effective, green and sustainable Federal cloud computing solutions.

- CC Standards WG Mission Statement:

Establish a framework and roadmap to drive standards to facilitate interoperability, portability, security and manageability for federal cloud computing services.

Federal vs. Commercial

Our Focus



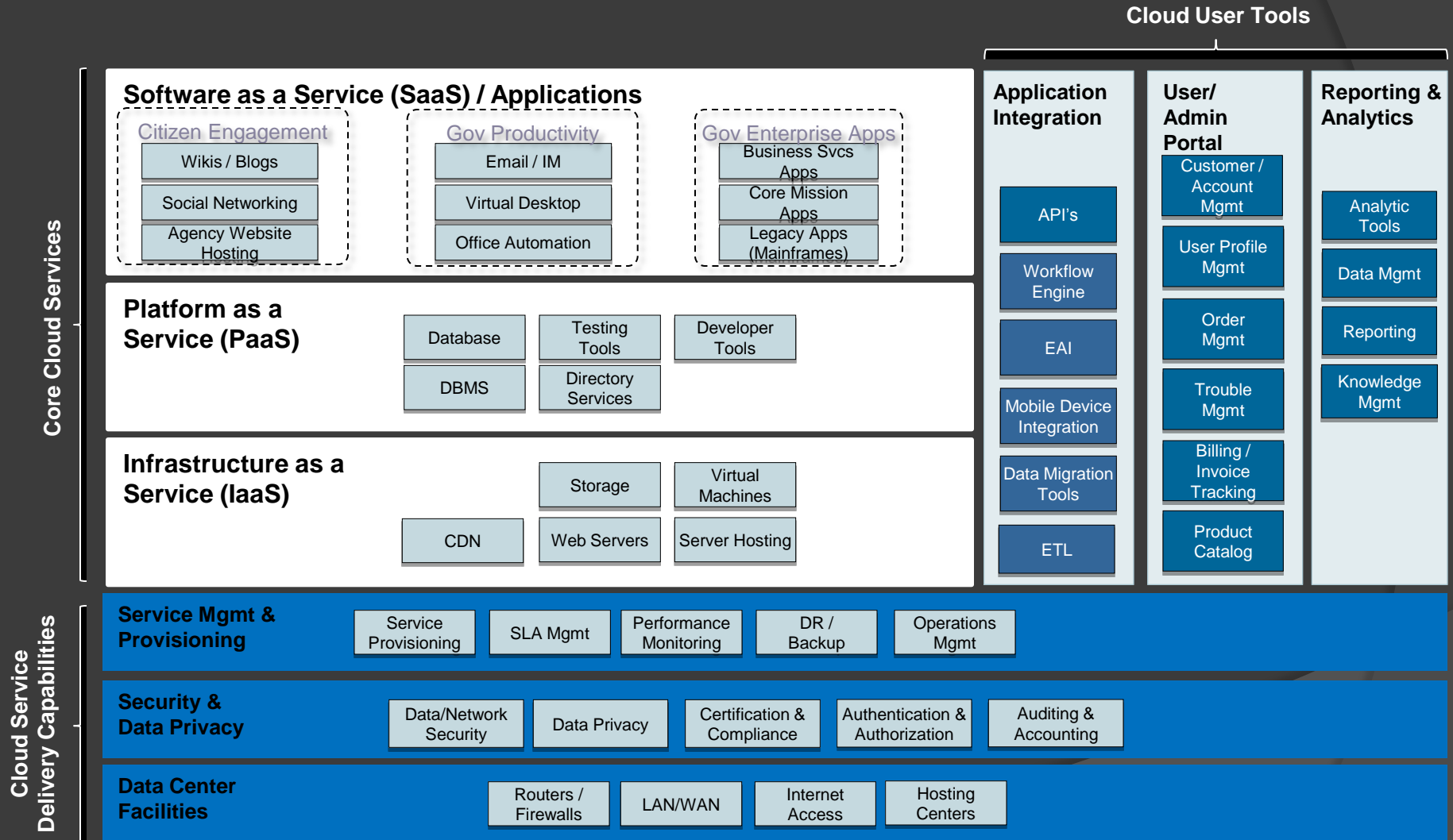
Federal
Requirements

Commercial
Requirements

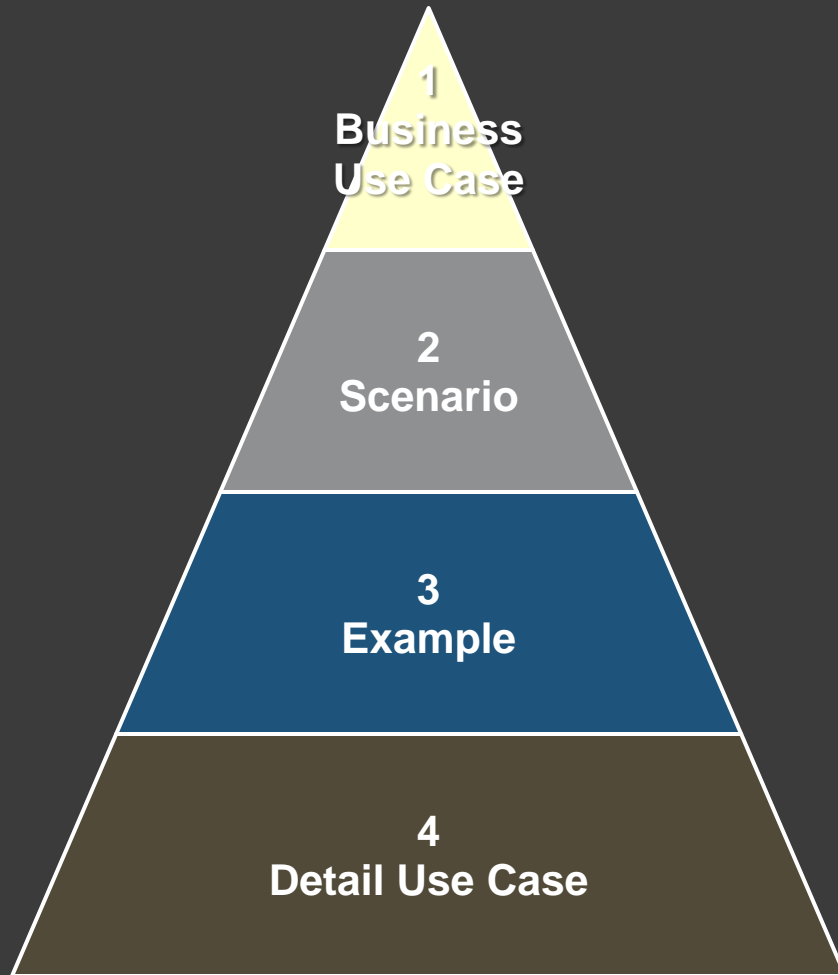
Goal of Federal Standards Activities

Provide guidance to industry and government for the creation and management of relevant cloud computing standards allowing all parties to gain the maximum value from cloud computing

Government Cloud Framework



Focus on Business Use Cases



Description	Focus
Business Use Cases present and describe a top level view of a category of related cloud business issues	Define boundaries and characteristics of a business focus area
Scenarios illustrate a particular facet of a business use case in order to highlight kinds of standards needed	Describe conditions for the scenario and the required kinds of standards to fulfill the need
Examples animate a scenario with a limited and specific case to illustrate practical implications of a scenario including references to potential standards implementations	Show how a scenario plays out in a real world situation with reference to existing standards where available
Detail Use Cases break down a scenario into actual functional components, tasks and activities. This is the traditional “programming” use case used in SDLC	Defines specific activities. NOT PART OF CURRENT DISCUSSION

Business Use Case 1: Initiating Cloud Service

Description	An agency wishes to initiate a new cloud service
Service Models	IaaS, SaaS, PaaS
Pre-conditions	None
Post conditions	Target services commissioned and provisioned
Key Considerations and Dependencies	Security policy specification including location dependencies Identity federation and management (All) Physical infrastructure selection, sizing and configuration (IaaS) Virtual Machine selection, sizing and configuration (IaaS) Storage selection, sizing and configuration (IaaS) Provisioning /deployment standards and specifications (IaaS, PaaS) Monitoring and management specification (All) Application and Document lifecycle specification (All) Platform selection and configuration specification (PaaS) Application selection and configuration specification (SaaS) Service Level specification and benchmarking (All)
References and Notes	Cloud Computing Use Cases Group 3.6.2 Grance, Mell (NIST) A Roadmap for Cloud Standards, 9/15/09

Conditions

- Agency wishes to establish an IaaS Service

Requirements

- Identity management standards to establish identity, authentication and authorization
- Security standards related to encryption, location-specific data storage, etc.
- Specification standards for physical boundaries, e.g. shared, dedicated or community pools of processors, networks, storage devices, etc.
- Specification standards for virtual resources including virtual machines, standard images, storage and virtual network configuration
- Provisioning standards to specify virtual resource elasticity parameters
- Monitoring and management standards for thresholds and controls
- Lifecycle standards for storage replication, retention and destruction
- Service level standards

Desired Results

- Essential portions of infrastructure are provisioned by standard specification

References and Notes

- Cloud Computing Use Cases Group 3.6.1
- Grance, Mell (NIST) A Roadmap for Cloud Standards, 9/15/09

Example 1.1.1 IaaS for Scientific Computing

Description

- Agency wishes to establish an IaaS Service for process-intensive scientific computing

Activities

- Authorized individual accesses an IaaS provider by preexisting account
- Declare identity domain by referencing established federated identities (SAML, WS-Federation, Liberty, ID-FF)
- Declare standards-based authorization /entitlement rules (XACML)
 - Declare key management and data encryption at rest and in flight (PKI, PKCS, KEYPROV (CT-KIP, DSKPP), EKMI)
- Declare physical boundaries: SPARC processors and SAN disk-accessible storage, drawn from community pool X only, shared machines and devices allowed (Standards do not exist)
- Define virtual resources:
 - Specify multicore high memory instances and large amounts of nonpersistent storage (Standards do not exist)
 - Select a vendor-specific virtual image (DMTF OVF) using a standard query and selection API (Standards do not exist) following risk based security standards (PCI-DSS)
 - Define a persistent storage structure and mapping (Amazon S3, GFS, Azure Storage, SNIA CDMI)
 - Define a VPN configuration (Amazon EC2)
- Declare provisioning rules (OGF OCCl, EC2 API)
 - Declare new instance spinup at 85% utilization of all running instances and termination at 20% utilization of any instance (Standards do not Exist)
 - Declare notification at 105 instances and notification and end of escalation at 150 (Standards do not Exist)
 - Declare data backup on a nightly basis to CONUS resource, and data destruction after 60 days (ISO 15489 but no implementation standards)
- Service level standards (Standards do not Exist)

References and Notes

- Grance, Mell (NIST) A Roadmap for Cloud Standards, 9/15/09

Business Use Case 2: Changing Cloud Vendors

Description	An agency wishes to migrate some or all of a set of existing cloud services to a new vendor
Service Models	IaaS, SaaS, PaaS
Pre-conditions	<ul style="list-style-type: none">• An existing set of cloud services with source vendor• A plan for replacement or migrated services with destination vendor
Post conditions	<ul style="list-style-type: none">• Source services decommissioned• Target services operating with minimal loss of data, security or business rule functionality
Key Considerations and Dependencies	Identity federation and management across vendors Security specification standards across vendors Industry-specific common standards for application types (SaaS) Platform standards and configuration (PaaS) Platform component (middleware) standards and configuration (PaaS) Application language standardization and portability (PaaS) Virtual machine standards, configuration and portability (IaaS) Storage standards and configuration (IaaS)
References and Notes	Cloud Computing Use Cases Group 3.6.2 Grance, Mell (NIST) A Roadmap for Cloud Standards, 9/15/09

Conditions

- Agency has an existing SaaS application and wishes to migrate all or part of it to a similar application with a new vendor

Requirements

- Identity management standards to migrate identity, authentication and authorization
- Security standards related to encryption, location-specific data storage, etc.
- Storage standards for migrating existing data
- Application-specific formatting standards for importing or reusing data
- Application-specific business rule standards (in some cases)
- Service level standards

Desired Results

- Users are able to access new application with appropriate permissions
- Migrated data is available within the defined security envelope
- Business rules are in operation on the target system

References and Notes

- Cloud Computing Use Cases Group 3.6.1
- Grance, Mell (NIST) A Roadmap for Cloud Standards, 9/15/09

Conditions

- Agency has an existing PaaS platform and wishes to migrate to a similar platform from another vendor ¹.

Requirements

- Include Identity, Security, Storage standards from 1.1
- Platform standards for configuring and managing platform operation and management
- Platform standards for configuring and managing application deployment
- Platform enabler standards for configuring and operating databases, message queues, service buses and related enablers

Desired Results

- Users are able to access new application with appropriate permissions
- Migrated data is available within the defined security envelope
- Business rules are in operation on the target system

References and Notes

- Cloud Computing Use Cases Group 3.6.2, 3.6.3
- Scope reduced to exclude migrations across dissimilar platform stacks ¹

¹ Similar platform refers to migration within similar PaaS stacks, e.g. LAMP to LAMP. JEE to JEE. .Net to .Net

Conditions

- Agency has an existing PaaS platform and wishes to migrate to a dissimilar platform from another vendor ¹.

Requirements

- Include all requirements from Scenario 1.2
- Language standards and cross-language portability standards or compatibility APIs
- Data management standards and API's to address different data models across platform, e.g. relational versus flat

Desired Results

- Users are able to access new application with appropriate permissions
- Migrated data is available within the defined security envelope
- Business rules are in operation on the target system

References and Notes

- Cloud Computing Use Cases Group 3.6.2, 3.6.3
- Grance, Mell (NIST) A Roadmap for Cloud Standards, 9/15/09

¹ Similar platform refers to migration within similar PaaS stacks, e.g. LAMP to LAMP. JEE to JEE. .Net to .Net

Business Use Case 3: Hybrid Cloud Operation

Description	An agency wishes to operate services across multiple clouds hosted by multiple vendors, potentially including private or community clouds
Service Models	IaaS, SaaS, PaaS
Pre-conditions	Services in multiple clouds with established SOA interoperability
Post conditions	Services interoperating across cloud boundaries
Key Considerations and Dependencies	Include: Business Case 1: Initiate Cloud Service Transactional and Concurrency standards Additional security standards for cross-cloud trust
References and Notes	Cloud Computing Use Cases Group 3.4.1. Note that Transactionality is excluded for Hybrid by CCUC but included here Grance, Mell (NIST) A Roadmap for Cloud Standards, 9/15/09

Business Use Case 4: Platform Configuration and Operation

Description	An agency wishes to configure a platform on which to develop, test or deploy SaaS applications
Service Models	PaaS
Pre-conditions	Available cloud infrastructure if required by the platform
Post conditions	Scalable platform available for development, testing or deployment of SaaS applications
Key Considerations and Dependencies	Include: Business Case 1: Initiate Cloud Service Platform standards and configuration (PaaS) Platform component (middleware) standards and configuration (PaaS) Application language standardization and portability (PaaS) Platform management and reporting standards (PaaS)
References and Notes	Grance, Mell (NIST) A Roadmap for Cloud Standards, 9/15/09

Next Steps

- ⦿ Federal Standards Web Workshop
 - Crowd-source ideas for roadmap
 - 3rd week of January
 - Open public invitation
- ⦿ Federal Standards Summit
 - April 2010
 - Present Federal Roadmap
 - Present Prioritized Federal Use Cases

Questions?

<http://nebula.nasa.gov>

Chris.C.Kemp@NASA.gov

twitter

@ChrisCKemp

@NASANebula